[**Application-Layer**](https://en.wikipedia.org/wiki/Application_layer)**Protocol Negotiation** (**ALPN**) is a [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS) extension that allows the application layer to negotiate which [protocol](https://en.wikipedia.org/wiki/Communications_protocol) should be performed over a secure connection in a manner that avoids additional round trips and which is independent of the application-layer protocols. It is needed by secure [HTTP/2](https://en.wikipedia.org/wiki/HTTP/2) connections, which improves the compression of web pages and reduces their latency compared to HTTP/1.x. The ALPN and HTTP/2 standards emerged from development work done by Google on the now withdrawn [SPDY](https://en.wikipedia.org/wiki/SPDY) protocol.



**Contents**

* [1Support](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#Support)
* [2History](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#History)
* [3Example](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#Example)
* [4References](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#References)
* [5External links](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#External_links)

Support[[edit](https://en.wikipedia.org/w/index.php?title=Application-Layer_Protocol_Negotiation&action=edit&section=1)]

ALPN is supported by these libraries.

* [GnuTLS](https://en.wikipedia.org/wiki/GnuTLS) since version 3.2.0 released in May 2013.[[1]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-GnuTLS-3.2.0-1)
* [MatrixSSL](https://en.wikipedia.org/wiki/MatrixSSL) since version 3.7.1 released in December 2014.[[2]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-MatrixSSL-3.7.1-2)
* [Network Security Services](https://en.wikipedia.org/wiki/Network_Security_Services) since version 3.15.5 released in April 2014.[[3]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-NSS-3.15.5-3)
* [OpenSSL](https://en.wikipedia.org/wiki/OpenSSL) since version 1.0.2 released in January 2015.[[4]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-OpenSSL-1.0.2-4)
* [LibreSSL](https://en.wikipedia.org/wiki/LibreSSL) since version 2.1.3 released in January 2015.[[5]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-libressl-2.1.3-5)
* [mbed TLS](https://en.wikipedia.org/wiki/Mbed_TLS) (previously PolarSSL) since version 1.3.6 released in April 2014.[[6]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-PolarSSL-1.3.6-6)
* [SChannel](https://en.wikipedia.org/wiki/SChannel) since 8.1 / 2012 R2.
* [s2n](https://en.wikipedia.org/wiki/S2n) since its original public release in June 2015.
* [wolfSSL](https://en.wikipedia.org/wiki/WolfSSL) (formerly CyaSSL) since version 3.7.0 released in October 2015. [[7]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-ChangeLog-7)
* [Go](https://en.wikipedia.org/wiki/Go_(programming_language)) (in the standard library crypto/tls package) since version 1.4 released in December 2014. [[8]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-go-1.4-8)
* picotls[[9]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-9)
* [JSSE](https://en.wikipedia.org/wiki/Java_Secure_Socket_Extension) in [Java](https://en.wikipedia.org/wiki/Java_(software_platform)) since JDK 9 released in September 2017.[[10]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-jsse-10), backported to JDK 8 released in April 2020. [[11]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-jsse2-11)
* [BearSSL](https://en.wikipedia.org/w/index.php?title=BearSSL&action=edit&redlink=1) since version 0.3 [[12]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-BearSSL-3.0-12)
* [Win32 SSPI](https://en.wikipedia.org/wiki/Security_Support_Provider_Interface) since Windows 8.1 and Windows Server 2012 R2 were released October 18, 2013[[13]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-Win32_SSPI-13)

History[[edit](https://en.wikipedia.org/w/index.php?title=Application-Layer_Protocol_Negotiation&action=edit&section=2)]

On July 11, 2014, ALPN was published as [RFC 7301](https://tools.ietf.org/html/rfc7301). ALPN replaces NPN [[14]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-14)

[TLS False Start](https://en.wikipedia.org/wiki/TLS_False_Start) was disabled in [Google Chrome](https://en.wikipedia.org/wiki/Google_Chrome) from version 20 (2012) onward except for websites with the earlier **Next Protocol Negotiation** (**NPN**) extension.[[15]](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_note-15)

Example[[edit](https://en.wikipedia.org/w/index.php?title=Application-Layer_Protocol_Negotiation&action=edit&section=3)]

ALPN is a TLS extension which is sent on the initial [TLS handshake](https://en.wikipedia.org/wiki/Transport_Layer_Security#TLS_handshake) 'Client Hello', and it lists the protocols that the client (for example the web browser) supports:

Handshake Type: Client Hello (1)

Length: 141

Version: TLS 1.2 (0x0303)

Random: dd67b5943e5efd0740519f38071008b59efbd68ab3114587...

Session ID Length: 0

Cipher Suites Length: 10

Cipher Suites (5 suites)

Compression Methods Length: 1

Compression Methods (1 method)

Extensions Length: 90

[other extensions omitted]

Extension: application\_layer\_protocol\_negotiation (len=14)

Type: application\_layer\_protocol\_negotiation (16)

Length: 14

ALPN Extension Length: 12

ALPN Protocol

ALPN string length: 2

ALPN Next Protocol: h2

ALPN string length: 8

ALPN Next Protocol: http/1.1

The resulting 'Server Hello' from the web server will also contain the ALPN extension, and it confirms which protocol will be used for the HTTP request:

Handshake Type: Server Hello (2)

Length: 94

Version: TLS 1.2 (0x0303)

Random: 44e447964d7e8a7d3b404c4748423f02345241dcc9c7e332...

Session ID Length: 32

Session ID: 7667476d1d698d0a90caa1d9a449be814b89a0b52f470e2d...

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)

Compression Method: null (0)

Extensions Length: 22

[other extensions omitted]

Extension: application\_layer\_protocol\_negotiation (len=5)

Type: application\_layer\_protocol\_negotiation (16)

Length: 5

ALPN Extension Length: 3

ALPN Protocol

ALPN string length: 2

ALPN Next Protocol: h2

References[[edit](https://en.wikipedia.org/w/index.php?title=Application-Layer_Protocol_Negotiation&action=edit&section=4)]

* 1. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-GnuTLS-3.2.0_1-0) [*"gnutls 3.2.0"*](https://web.archive.org/web/20160131230710/http:/article.gmane.org/gmane.network.gnutls.general/3136)*. Archived from*[*the original*](http://article.gmane.org/gmane.network.gnutls.general/3136)*on 2016-01-31. Retrieved 2015-01-26.*
  2. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-MatrixSSL-3.7.1_2-0) [*"MatrixSSL - News"*](https://web.archive.org/web/20150214105056/http:/www.matrixssl.org/news.html)*. 2014-12-04. Archived from*[*the original*](http://www.matrixssl.org/news.html)*on 2015-02-14. Retrieved 2015-01-26.*
  3. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-NSS-3.15.5_3-0) [*"NSS 3.15.5 release notes"*](https://developer.mozilla.org/en-US/docs/NSS/NSS_3.15.5_release_notes)*. Mozilla Developer Network. Mozilla. Retrieved 2015-01-26.*
  4. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-OpenSSL-1.0.2_4-0) [*"OpenSSL 1.0.2 release notes"*](https://www.openssl.org/news/openssl-1.0.2-notes.html)*. The OpenSSL Project. The OpenSSL Project. 2015-01-22. Retrieved 2015-01-26.*
  5. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-libressl-2.1.3_5-0) [*"LibreSSL 2.1.3 released"*](https://marc.info/?l=openbsd-announce&m=142193407304782)*. 2015-01-22. Retrieved 2015-01-26.*
  6. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-PolarSSL-1.3.6_6-0) [*"Download overview - PolarSSL"*](https://polarssl.org/tech-updates/releases/polarssl-1.3.6-released)*. 2014-04-11. Retrieved 2015-01-26.*
  7. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-ChangeLog_7-0) [*"wolfSSL Release Change Log"*](https://www.wolfssl.com/wolfSSL/Docs-wolfssl-changelog.html)*. 2015-10-26. Retrieved 2015-09-11.*
  8. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-go-1.4_8-0) [*"Go 1.4 Release Notes"*](https://golang.org/doc/go1.4#minor_library_changes)*. 2014-12-10. Retrieved 2017-11-28.*
  9. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-9) [*"Picotls"*](https://github.com/h2o/picotls/blob/master/include/picotls.h#L510)*. Github. Retrieved 2 August 2018.*
  10. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-jsse_10-0) [*"JEP 244: TLS Application-Layer Protocol Negotiation Extension"*](https://bugs.openjdk.java.net/browse/JDK-8051498)*. 2017-08-07. Retrieved 2018-08-29.*
  11. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-jsse2_11-0) {{cite web|title=Release Note: TLS Application-Layer Protocol Negotiation Extension|url=[https://bugs.openjdk.java.net/browse/JDK-8242894%7Cdate=2020-04-30%7Caccessdate=2020-06-11}](https://bugs.openjdk.java.net/browse/JDK-8242894%7Cdate=2020-04-30%7Caccessdate=2020-06-11%7D)
  12. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-BearSSL-3.0_12-0) [*"BearSSL - Changelog"*](https://bearssl.org/changelog.html#version-0.3)*. Retrieved 2010-09-08.*
  13. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-Win32_SSPI_13-0) [*"What's New in TLS/SSL (Schannel SSP)"*](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831771(v=ws.11)?redirectedfrom=MSDN#whats-new-in-tlsssl-schannel-ssp-in-windows-server-2012-r2-and-windows-81)*. Retrieved 2020-03-30.*
  14. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-14) *Langley, Adam.*[*"» NPN and ALPN"*](https://www.imperialviolet.org/2013/03/20/alpn.html)*. Retrieved 2 April 2013.*
  15. [**^**](https://en.wikipedia.org/wiki/Application-Layer_Protocol_Negotiation#cite_ref-15) *Langley, Adam.*[*"False Start's Failure (11 Apr 2012)"*](https://www.imperialviolet.org/2012/04/11/falsestart.html)*. Retrieved 25 September 2013.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=Application-Layer_Protocol_Negotiation&action=edit&section=5)]

* [The registry of ALPN protocol IDs is maintained by IANA as a TLS extension.](https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml#alpn-protocol-ids)
* [draft-agl-tls-nextprotoneg-04 (NPN draft)](https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04) (last updated: May 2012)
* [RFC 7301](https://tools.ietf.org/html/rfc7301) "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension"